Intel® Advanced Digital Set Top Box Design

White Paper: Techniques and Approaches for Security Robustness Rules

September 2003

Revision 1.0

Order Number: 273967

Contents

Figures

Tables

§ §

1.0 Introduction

Intel® Advanced Digital Set Top Box Design (ADSTB) is a design based on Intel and third-party silicon. As a very general statement, a commercial Advanced Digital Media Center Set Top Box (hereafter referred to as STB) must be designed in a manner that frustrates attempts by casual users or hackers to intercept and/or make copies of protected content except as authorized by the rights holder. Specific standards of "robustness" are found in the specific licensing agreements associated with particular technologies, such as DTCP, CPPM, and CSS. It is critical for designers to understand how content protection policies for digital television content affects hardware and software design. A STB must be designed such that copyrighted content received from a protected digital input is transferred or stored within the STB in a robust manner, output to a display, or distributed robustly to another STB or Thin Client (example: Digital Media Renderer) within the home.

The Intel® ADSTB main board design is a flexible and modular development platform but does not address all possible content security risks. This white paper provides references to content protection technologies, techniques and approaches for designing a robust set top box that is based on the Macks Canyon design design. It may be used by hardware and software designers to incorporate content protection in their own STB designs. While this white paper outlines various approaches that may be considered, the ultimate design decisions are the responsibility of the implementer, who should carefully study the specific robustness requirements associated with the technology being implemented.

2.0 Overview of Content Protection Technologies

2.1 Conditional Access

Conditional Access is a term applied to the set of technologies that allow a service provider to prevent unauthorized users from gaining access to restricted cable content. Some form of Conditional Access (CA) is usually applied at the service provider head-end prior to distribution of premium content over satellite and cable. Service providers typically partner with CA vendors who provide a solution for key management, content scrambling at the distribution head-end and a subscriber management system. At the receiver, a CA vendor's client software is employed to extract the scrambling key and de-scramble the encrypted content. The CA client software uses elements that are designed into the hardware or the media processor itself, such as a de-scrambler engine and interfaces for removable CA tokens, such as a smart card, OpenCable™ POD or DVB-CI module.

Service providers typically partner with CA vendors who provide a solution for key management, content scrambling at the distribution head-end and a subscriber management system. At the receiver, a CA vendor's client software is employed to extract the scrambling key and de-scramble the encrypted content. The CA client software uses elements that are designed into the hardware or the media processor itself, such as a de-scrambler engine and interfaces for removable CA tokens, such as a smart card, OpenCable™ POD or DVB-CI module.

The broadcast standard defines the scrambling algorithm and a framework for CA to be implemented in the receiver. This allows designers to design systems that implement the basic CA elements in hardware. Each CA vendor may also have specific requirements to be implemented in hardware, beyond the basic CA elements defined in a given broadcast standard. Note that the broadcast standard does not define the details of how CA is implemented. This is left to the specific CA vendor and is typically implemented in CA client software running on the media processor in

conjunction with a CA token that is given to the subscriber. The CA token may take the form of a smart card that has to be inserted into the STB or a CA module that resembles a PCMCIA card Table 1 lists the CA scrambling algorithm for each broadcast standard.

The Intel® ADSTB design may need to be modified to adapt the design to a specific CA solution.

Table 1. Conditional Access Overview

Conditional Access for Satellite		
Broadcast Standard	**CA De-scrambling Algorithm Defined by the Standard**	**CA Token**
DVB-S	DVB-CSA (Content Scrambling Algorithm) available under license from DVB.	Smart card or DVB-CI compliant, removable CA module depending on the specific CA vendor's solution adopted by the service provider.
DSS (DirecTV)	DES. Need DirecTV license	Smart card
ARIB	MULTI-2 (ARIB B-25 specification)	Smart card
Conditional Access for Cable		
Broadcast Standard	**CA De-scrambling Algorithm Defined by the Standard**	**CA Token**
DVB-C	Same as DVB-S	Smart card or DVB-CI compliant, removable CA module depending on the specific CA vendor's solution adopted by the service provider.
OpenCable™ (North America)	DES/DFAST	CableCARD™ (previously known as POD – Point of Deployment system).
Motorola CATV (USA)	DES/Digicipher II	N/A
Scientific Atlanta CATV (USA)	DES/PowerKey	N/A

2.2 Content Protection Technologies

Premium content is delivered in an encrypted form to a receiver device, protected either by conditional access (usually for content broadcast over satellite/cable) or some other digital rights management (DRM) solution for Internet delivered content.

There are several content protection technologies available today to protect entertainment content as it is delivered, stored, transferred and displayed within an entertainment device or between devices within the home. The 4C entity is an industry group formed by Intel, IBM, Matsushita and Toshiba with the goal of developing technologies that contribute to a comprehensive content protection solution. The CPSA (Content Protection System Architecture) white paper [1] by the 4C entity describes an overall framework to protect entertainment content as it passes from one technology to another within the content protection ecosystem. This CPSA white paper is a good reference (see Section 9.0, "References") for designers to gain an understanding of how compliant devices handle copy control information, playback, output and recording. It is necessary to employ content protection technologies for both analog and digital domains.

A summary of these technologies is given in Table 2.

Table 2. Summary of Content Protection Technologies

Solution	Applicable to	Summary
CA (Conditional Access)	Copyrighted content distributed, typically by satellite or cable.	An overview of CA is discussed in Section 2.1. A CA scheme is specific to a CA vendor that is chosen by a service provider to protect its broadcast content.
CSS	Pre-recorded video on DVD-ROM	Content Scramble System (CSS) defines the technology for how DVD movies are encrypted by manufacturers and the decryption mechanism in hardware or software players. See [7] in Section 9.0.
CPPM	Audio on DVD-ROM	Content Protection for Pre-recorded Media (CPPM) and Content Protection for Recordable Media (CPRM) are technologies licensed by 4C Entity LLC (developed by IBM, Intel, MEI, and Toshiba). See http://www.4centity.com for details.
CPRM	Audio/Video on DVD-R/RW/RAM	
DTCP	IEEE 1394, USB, IP networks (Q3, 2003)	Digital Transmission Content Protection (DTCP) defines a cryptographic protocol for protecting A/V content over high performance digital buses such as IEEE 1394, USB and IP networks. See http://www.dtcp.com for further information.
HDCP	Digital Visual Interface (DVI) and High Definition Multimedia Interface (HDMI	High-bandwidth Digital Content Protection (HDCP) is a technology developed by Intel Corporation to protect digital entertainment content (uncompressed pixel data at screen refresh rates) across the DVI or HDMI interconnect between a digital display device and a content renderer. See http://www.digital-cp.com for further information.
CGMS-A	Analog NTSC video	This standard defines copy protection capabilities for analog NTSC video by extending the EIA-608 standard to control Macrovision's Analog Copy Protection (ACP) anti-copy process at the receiver. EIA-608 defines closed captioning and other extended data services in the line 21 (vertical blanking interval) of the analog NTSC signal.
Macrovision ACP	Analog video that is output from DVD players and other devices such as analog display of pay-per-view content.	Analog Copy Protection (ACP) is a proprietary system developed and patented by Macrovision. When applied to the digital to analog conversion process in the receiver (such as a DVD player) the analog output is viewable on a television set but prevents copying by VCR. See http://www.macrovision.com for more information.

2.3 Robustness Rules

Once content that is protected by a CA solution or some other form of DRM is de-scrambled (or unencrypted) in a receiver, the unencrypted digital content may be vulnerable to unauthorized interception and copying by hackers. "Robustness rules" define the rules for how the internal design of a receiver protects the content flow within the receiver system but do not dictate how specific implementations must satisfy those rules. Complying with robustness rules generally result in solutions aimed at both casual and seasoned hackers.

Robustness rules may be derived from the following sources of information:

1. Robustness rules from DTCP licenses

   Platform robustness rules are specified in some industry content protection technology license requirements. Digital Transmission Control Protocol (DTCP [1]) put forth by the DTLA (also known as 5C) deals with the secure re-distribution of content over high-speed networks within the home. Although DTCP deals with the secure distribution of content, the DTCP license (see [2]) describes robustness requirements within the box in great detail.

2. HDCP [5] defined by Digital Content Protection, LLC is a technology for protecting high definition digital content between a receiver and a digital HDTV. The HDCP license also includes robustness rules in Exhibit D of the license agreement.
3. CableLabs® through its OpenCable™ project has defined a Host-POD specification for connecting POD modules to set-top terminals for authorizing and descrambling programs in the receiver. In addition, CableLabs® has also defined a specification for protecting the content sent across this interface, which includes the DFAST scrambling techniques. The Host-POD specification, called PHILA (POD-Host Interface License Agreement [8]) includes a set of robustness rules in Exhibit B that must be met by the cable receiver system.
4. Customer requirements: Service providers and Consumer Equipment (CE) manufacturers may have their own requirements and schemes for robustness within the box, in addition to those required by the above-mentioned technology licenses.
5. Industry white papers: Intel has published white papers on this topic (see references [3] and [4]).
6. For media delivered via the Internet, the conditional access (restriction of content usage to specific users) is usually encapsulated within the DRM solution being used The DRM solution provider may also impose some platform security requirements.

Note: Although the DTCP standard deals with the secure distribution of content, the DTCP license (see [2]) describes robustness requirements within the box in great detail. Exhibits B and C (Robustness rules, page 35) of the DTCP license are good references for ‘internal’ robustness requirements.

3.0 Summary Of Robustness Rules

DTCP [2], HDCP [5] and PHILA [8] license requirements have several compliance and robustness rules that state how content is to be stored and distributed within the STB. In addition, conditional access license, DRM providers and service providers may have their own requirements for content protection.

Designers must thoroughly understand the content protection requirements outlined in the license documents and their own customer requirements and incorporate them into the design process. DTCP and HDCP licenses provide a questionnaire, which designers may use to determine whether their platform complies with the standard. Use of this questionnaire as a checklist does not necessarily ensure compliance of the final product, but it is a convenience tool for the designer to gauge the general robustness of their design against. Key points of the robustness rules are summarized below.

1. **Avoid defeating functions:** A robust set top box must not include switches or jumpers on the board or configuration menus or options in software that allow the set top box to operate in an “unprotected” mode. An unprotected mode is entered when content protections are defeated or turned off and decrypted content or data is exposed to unauthorized interception and/or copying by a user. If there are means in software to turn off protection systems, the license requires the adopter to clearly specify what steps have been taken to ensure that these options will not be used to defeat the content protection. User discretion is not an option.

2. **Avoid unencrypted digital content flow on user-accessible buses:** Unencrypted digital content, which was originally received into the STB encrypted, must not flow over user-accessible buses within the system. Thus, once the digital content is decrypted within the STB, content protection must be implemented in hardware, software or a combination to prevent its unauthorized interception or copying. The definition of a 'user-accessible bus' is spelled out in both the DTCP and HDCP license robustness rules section. Section 2 of Exhibit C (Robustness Rules) of the DTCP license [2] explains this in detail.
3. **Protect sensitive material:** Sensitive cryptographic material such as encryption keys and other confidential material specified by the licensing authority must be stored on the system, in a manner that is designed to effectively frustrate attempts to discover or reveal them. Section 1.3 and 3.5 of Exhibit C (Robustness Rules) of the DTCP license [2] explains this in detail. In addition, algorithms employed in software should use code obfuscation techniques such as Tamper Resistant Software solutions available from third parties to protect the confidential material such as coefficients and intermediate calculations that could compromise the security of the system if discovered. Section 3 of Exhibit C (Robustness Rules) of the DTCP license [2] explains this further.
4. **Ensure System Integrity**: Section 3.2.2, Exhibit C or the DTCP license [2] requires that DTCP licensed systems be designed to perform self-checking of the integrity of its software and hardware components such that unauthorized modifications results in failure of the system to operate.

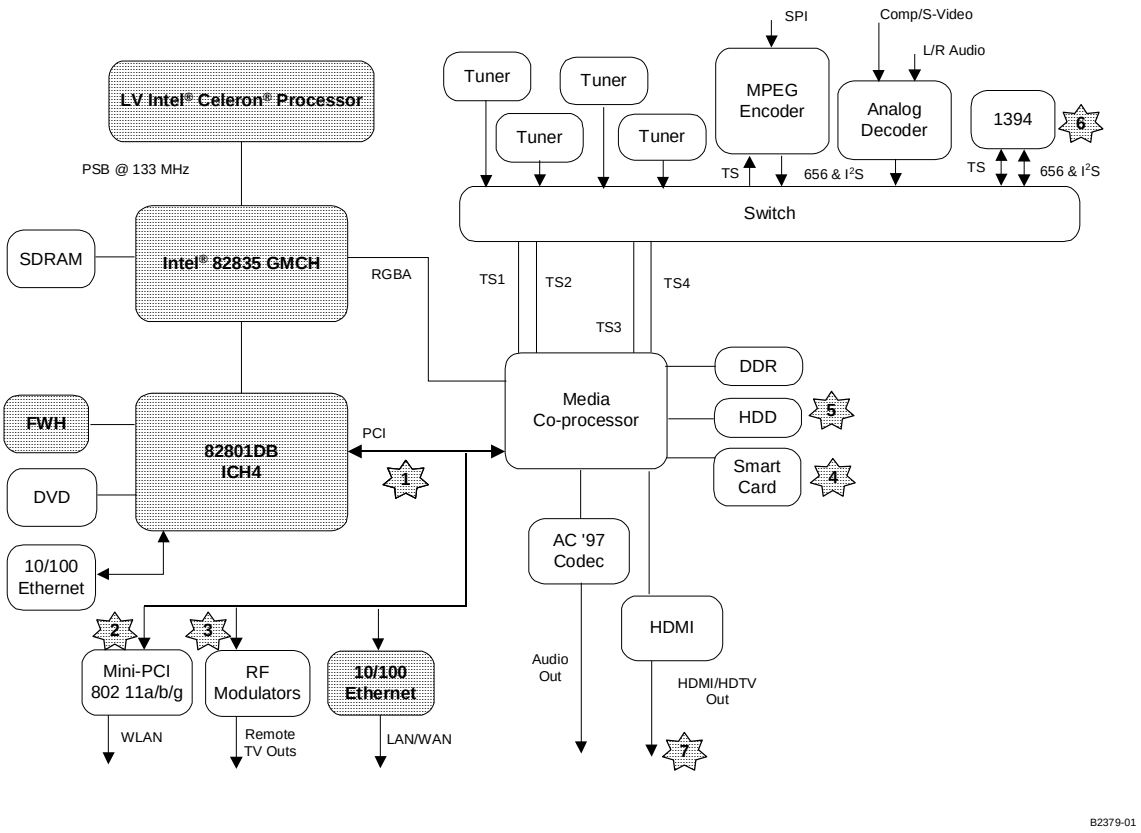
Specific recommendations to address these robustness rules for the Intel® ADSTB design are provided in Section 5.0.

4.0 Robustness Analysis of Internal Buses

In general, the robustness rules define what security holes the design should prohibit but do not provide any implementation details. There are a number of possible approaches and techniques that might be used to meet the robustness rules, each with varying degrees of robustness. The final choice of the solution is left to the designer/manufacturer based on their own customer requirements and legal/technical analysis.

Figure 1 shows the internal architecture of the Intel® ADSTB design. Each internal bus that supports protected content flow is identified with a number and Table 3 provides an analysis of the robustness concerns associated with these buses. A robustness concern usually arises if a bus is user-accessible and unencrypted, compressed content or unencrypted keys are transferred over it. Designers must consult the appropriate license agreements for robustness rules and definitions of what is considered a "user-accessible" bus. According to the DTCP license agreement, Exhibit C, a "user-accessible" bus means (a) an internal analog connector that: (i) is designed and incorporated for the purpose of permitting end-user upgrades or access or (ii) otherwise readily facilitates end user access or (b) a data bus that is designed for end user upgrades or access. Examples of user-accessible buses are implementations of smart cards, PCMCIA, Cardbus or PCI that have standard "user upgrade" sockets or otherwise readily facilitates end-user access. Memory buses, CPU buses or similar portions of a device's internal architecture that do not provide access to content in a form usable by end-users are not considered user-accessible.

Figure 1. Intel® Advanced Digital Set Top Box Design Block Diagram



NOTE: Refer to Table 3 for legend information.

Table 3. Security Analysis of Internal Buses

Figure 1 Marker Number	Bus	Security Concern
1 & 2	PCI bus / mini-PCI	The PCI bus is considered a “user-accessible bus” by default and only encrypted content must flow over it. Special considerations need to be given to designs that include a RF re-distribution solution that relies on content transferred over the PCI bus or a mini-PCI slot for wireless LAN distribution. These issues are discussed in detail in the next section.
3	Input to RF modulator	In the design, the RF modulator is an add-in removable card on the PCI bus. The add-in nature of this card makes it possible to intercept the unencrypted content flowing to it and therefore presents a robustness issue. The RF modulator module is discussed in detail in the next section.
4	Smart Card interface (ISO 7816)	This may be considered a user-accessible bus because a removable smart card is typically used with this interface. Sensitive data is exchanged with the smart card by the conditional access software client running on the media processor. The CA client software usually encrypts sensitive data that is sent across this interface to the smart card. In the case of OpenCable™-compliant designs, the PHILA license governs the use of DFAST scrambling technology to secure the traffic across the Host-POD interface.
5	Hard Disk Drive (HDD) – IDE Interface	Commercial content recorded by a PVR application to the HDD needs to be encrypted as defined by the DTCP compliance rules, Digital Rights Management, or Conditional Access license requirements.
6	IEEE-1394	Digital content that is output over the IEEE-1394 interface must be protected using DTCP unless the copy control information for the content does not impose any copy restrictions. See DTCP license Exhibit B for details.
7	Digital input to HDMI/DVI	Content must be protected over the DVI or HDMI interface with HDCP. If content is passed from the video decoder to the DVI / HDMI driver unencrypted, the content must be protected in some other way, such as hiding traces on inner layers to prevent interception.

5.0 Intel® Advanced Digital Set Top Box Design - Robustness Rules Considerations

This section provides suggestions for incorporating robustness rules into a Media Center Set Top Box based on the Intel® ADSTB design. Designers may need to implement one or more of these solutions into their designs based on platform configuration and customer requirements.

5.1 Protecting Content over User-accessible Buses

Buses such as the PCI bus that are non-proprietary in nature have the possibility of carrying unencrypted content between sub-systems. They are user-accessible and vulnerable to unauthorized content interception.

5.1.1 Encrypting Content Flows over “User-accessible” Buses

The most straightforward technique to protect the flow of content over user-accessible buses between nodes within the system is to always send encrypted content. This solution requires that each endpoint have the following:

- Crypto engines implemented in hardware or software at both endpoints that encrypt/decrypt data using a robust cipher such as Advanced Encryption Standard (AES) [6].
- The crypto engines at both endpoints also need to implement an effective key management strategy so that the key(s) used to encrypt and decrypt the data are securely shared between the two endpoints.

Section 7.0 explores this solution in greater detail.

5.1.2 Making the Bus Inaccessible

Another technique that may be employed to protect the unencrypted content flow over a user-acessible bus is to simply make the bus non-accessible to any user. Using such defensive board layout techniques may be considered as mitigation techniques in those instances where it is deemed sufficient to fulfill specific license obligations, as outllined in the following sections.

5.1.2.1 Defensive Board Layout Techniques

1. Do not provide any end-user upgrade slots on buses that could be classified as user-accessible.
2. Hide as many traces of such buses in inner layers of the board as possible.
3. Use a BGA or CSP package type for integrated circuits connected to this bus. BGA and CSP package types do not expose the IC pins on the side or top of the package, making it harder to tap into signals. If leaded packages must be used, epoxy or some other material must be placed on top of the part to prevent probing of the pins.

Designers are encouraged to follow all of the above recommendations when this approach is deemed suitable to meet the specific requirements of a specific technology license. It is not likely to ever be sufficient, however, to only follow recommendation 1 (no upgrade slots). While this protects against a casual hacker making illegal copies of protected content using an add-in card, it is not likely to protect the receiver against attacks from seasoned hackers, and robustness rules generally outline rules aimed at both casual and seasoned hackers. A more robust solution must also hide as many traces of the vulnerable bus as possible and use BGA packages for devices that are attached to the bus.

5.1.3 Securing the RF Modulator Board

The RF modulator board in the design is a PCI card that plugs into the main board through a riser card that electrically connects to the PCI bus. The current PCI card receives unencrypted MPEG-2 transport streams from the media co-processor over the PCI bus, decodes the streams using a Sigma 8470 decoder and performs the analog re-modulation for distribution over coaxial cable to televisions in the home.

An example of the content flow between the media processor and the RF modulator is the viewing of content stored by a PVR application on the hard disk attached to the media co-processor’s IDE bus. The content flow in this example is as follows:

1. The AES encrypted MPEG-2 transport stream is read in chunks off the content file stored on the hard disk and decrypted into the media co-processor local memory.

2. The decrypted buffers are transferred using DMA from the media co-processor local memory into the IA-32 memory buffer and then pushed to the Sigma 8470 decoders on the PCI card over the PCI bus.
3. The content buffers are decoded by the MPEG-2 decoder chip on the add-in card and then modulated for analog distribution over the coaxial cable.

In step 2., the content is sent unencrypted over the PCI bus. If the PCI bus is user-accessible, there is a robustness issue and a failure to comply with the 5C robustness rules. There are two cases to consider for the RF modulator board.

5.1.3.1 Case A: RF Modulator without AES Decryption Capability

In this case, the RF modulator design does not have AES decryption capability. Hence, the MPEG-2 transport stream is transferred unencrypted over the PCI bus between the media co-processor and the RF modulator daughter card.

1. To protect the unencrypted flow, it is important to make the PCI bus user-inaccessible by at least following the recommendations outlined in the earlier section. In addition, it is advisable to embed the PCI card circuitry onto the main board itself (no add-in card) and hide as many PCI traces as possible.
2. Assuming that the PCI card circuitry is placed on the main board and traces are hidden, there is still another possible robustness issue – a mini-PCI slot. The PCI bus must ideally not have an accessible mini-PCI connector (for example, to plug in a 802.11 wireless LAN module) because this makes it possible to plug in a card that can snoop signals on the PCI bus and intercept unencrypted content flow. If a mini-PCI connector is provided, designers must consider some other means to make the PCI bus inaccessible. See Section 5.1.4 for suggestions to the development of possible solutions.

5.1.3.2 Case B: RF Modulator with AES Decryption Capability

In this case, the RF modulator PCI card uses a part that has AES decryption capability. The AES-encrypted PVR content could be read off the hard disk and transferred encrypted over the PCI bus to the PCI card without being decrypted in the media co-processor part.

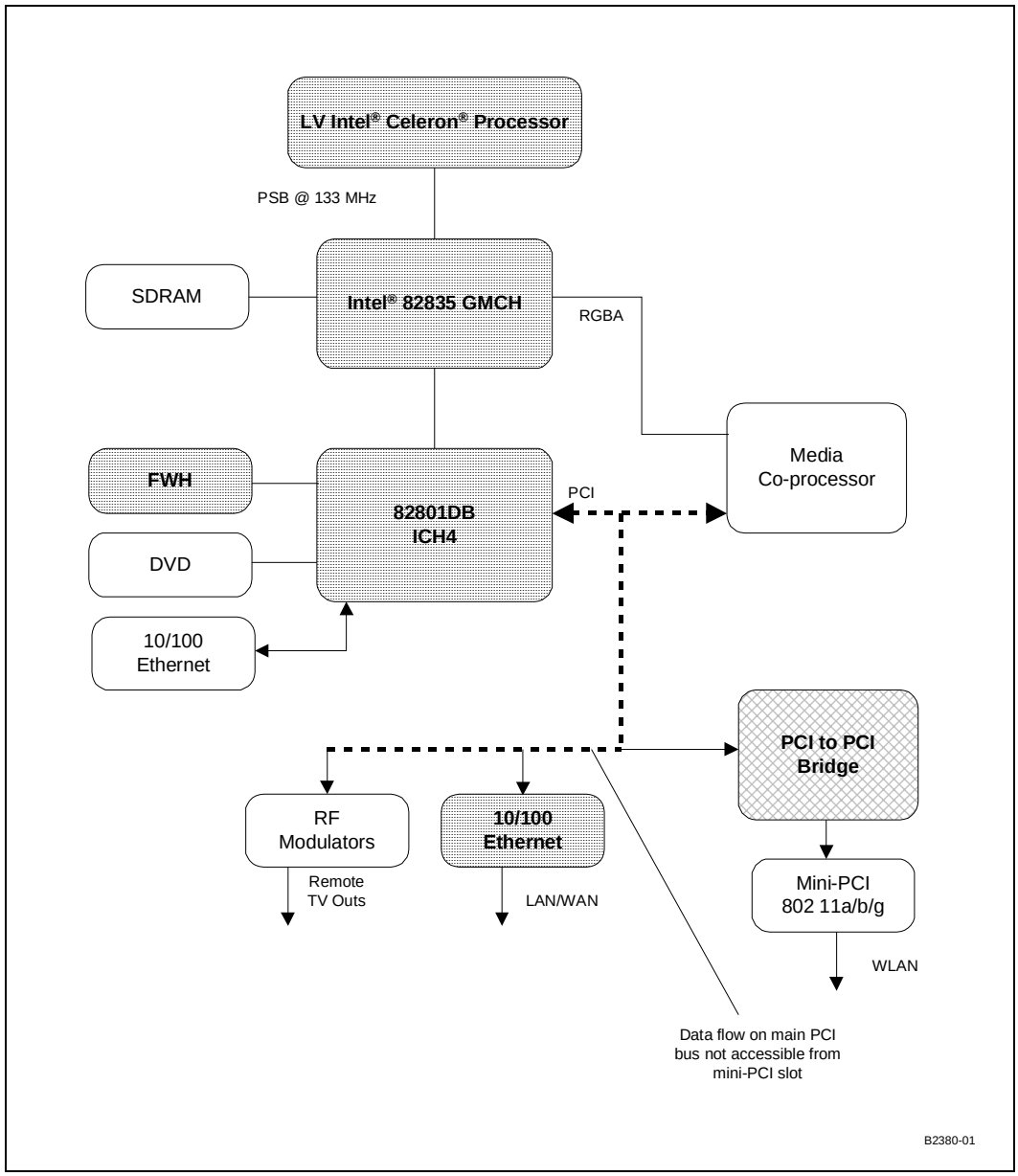
1. This solution provides a more robust means for transferring content between the media co-processor and the RF modulator on the PCI bus than the case discussed in Section 5.1.3.1, because only encrypted content appears on the PCI bus. This also highlights one of the benefits of using encryption whenever a user-accessible bus will be encountered. If content is always sent encrypted over the PCI bus, this allows the flexibility of providing a mini-PCI connector on the PCI bus without necessarily employing some of the techniques outlined in Section 5.1.2. The user-accessibility of the PCI bus is then also less of a concern in this case.

2. The AES decryption engine in the RF modulator PCI card needs to be programmed with the key that will be used for decrypting the content. It is important that the key is not transferred in the clear over a user-accessible PCI bus, especially if the RF modulator is a plug-in PCI card or the PCI bus is otherwise user-accessible. A secure key exchange or pre-shared key mechanism needs to be employed between software running on the IA-CPU or media co-processor and the AES decryption engine on the RF modulator.

5.1.4 Securing the Mini-PCI Slot

A mini-PCI slot on the PCI bus is a robustness concern for designs where unencrypted content is sent from the media co-processor to the IA CPU or the RF modulator board (as described in Section 5.1.3) over a PCI bus, even if defensive board layout techniques have been employed to make the PCI bus inaccessible. This is true because the mini-PCI slot essentially makes the PCI bus signals accessible. This again highlights the benefits of encrypting the content whenever a user-accessible bus might be encountered. An example where content is sent over the PCI bus from the media co-processor to the IA CPU is when content is to be distributed to remote thin clients over an IP network. Software running on the IA CPU in this case would act as a DTCP source device, encrypting and formatting the content data to be sent to the remote DTCP sink device.

Figure 2. PCI-to-PCI Bridge for Isolating the Mini-PCI Slot



5.1.4.1 Techniques

1. Send only encrypted content over the PCI bus. This implies that encrypted PVR or time-shifted content read off the hard disk attached to the media co-processor is not decrypted in the media co-processor. Instead, the data is sent encrypted into buffers in IA memory over the PCI bus. The AES decryption of this data is done in software on the IA CPU. This scheme requires a key management solution to be put in place so that keys are securely exchanged or pre-shared between software modules running on the IA CPU and the media co-processor. **Other techniques described in the following may mitigate the risks but should not be adopted as solutions themselves. These are offered as ideas for consideration.**

2. Design the mini-PCI add-in card functionality down on the main board if possible.
3. Isolate the mini-PCI slot to a secondary PCI bus by using a PCI-to-PCI bridge device as shown in Figure 2. Use PCI bridge device that is available as a BGA package to prevent interception of signals at the pins of the chip.
4. Instead of a mini-PCI slot, consider using an internal USB wireless LAN adapter connected to the USB port provided by the ICH4. This allows the PCI bus traces to be hidden and thus completely non-accessible.

5.2 Providing Secure Storage of Sensitive Materials

The Intel® ADSTB design includes flash memory connected to the media co-processor that is used as the boot ROM device for the media co-processor. This flash memory can also be used for storage of PVR encryption key(s), digital certificates, DTCP or other license keys and other sensitive material.

1. Keys cannot be stored in the clear in flash. The keys stored in flash device must themselves be encrypted with a 'key encryption key' (KEK) so that the keys cannot be read out of the flash device by a hacker. When keys are stored encrypted, they need to be read from the flash device by software and decrypted before being used. The KEK can be compiled into code and hidden in the binary by using code obfuscation techniques such as TRS (Tamper Resistant Software). TRS solutions are available from third parties.
2. Keys should not be stored on the hard disk along with the encrypted content unless the key is encrypted using a robust algorithm and the KEK is protected by TRS.

5.3 Ensuring System Integrity

5.3.1 Performing System Integrity Checks

In most designs, the system flash device is likely to be used for storage of certificates and encrypted keys. The system should be designed to perform self-checking of the integrity of its critical components such that unauthorized modifications result in failure of operation.

Techniques

1. To ensure that the system flash device is not tampered with, the BIOS boot code should verify the signature of the flash image on startup.
2. In addition, the BIOS boot code should check the integrity of compressed kernel image and/or application files to prevent unauthorized modifications to the system.
3. Applications implementing parts of a content protection scheme should be tamper resistant and/or employ some self-checking mechanism to check the integrity of the binary image.

5.3.2 Allowing Only Secure Software Updates

Software updates to the BIOS, kernel or application software should use a mechanism that ensures that only signed code can be downloaded and installed on the system.

5.3.3 Including Intrusion Detection

Incorporating an intrusion detection system into the platform is the first line of defense at attempts by hackers to compromise the security of the system. An effective intrusion detection system that renders a tampered platform inoperable turns the set top box into a 'closed system.' Intel recommends using intrusion detection in conjunction with other solutions suggested earlier to build a more robust system.

The Intel® ADSTB design has an intrusion detection mechanism to flag software when the chassis has been opened. The design consists of a header which may be attached to a chassis-mounted micro-switch or photodiode. The header connects to the I/O Controller Hub 4 (ICH4) INTRUDER# signal, which is powered from the RTC well, ensuring that the intrusion status will be preserved even if the power has been removed from the system.

If INTRUDER# is asserted the INTRD_DET bit in the TCO_STS register is set. This can enable the ICH4 to drive an SMI# or interrupt. Software can then read this bit to determine if the chassis has been opened, indicating potential tampering with the system.

6.0 Security Considerations for Personal Video Recorder Applications

Personal Video Recorder (PVR) applications provide users with the ability to have time-shifted playback of received content, i.e., the ability to pause and resume playback. In addition, PVR applications allow users to record content on internal storage (hard disk drive) for later viewing.

Designers of receivers that include the PVR feature must pay close attention to the following considerations.

1. The PVR application must follow the Copy Control Information (CCI) or "Usage Rules" that define constraints specific to making copies of the copyrighted content. CCI is either embedded in some form in the content itself, defined by licensing rules, or implied by the type of content being recorded. For example, DTCP compliance rules define how DTCP source and sink devices must treat CCI information for content delivered or received as DTCP encrypted data. Conditional Access license agreements, DRM licenses and other legal agreements may dictate CCI rules as well.

   Content must not be transferred, copied or stored except as allowed by CCI rules. PVR applications must cache content only as allowed and for the duration allowed.

2. Unless the CCI information specifies that copies can be made freely, content recorded to internal storage by PVR applications must be protected using an encryption protocol that ensures that the encrypted content is essentially bound to the licensed system and cannot be played back on another device or useable copies made except as permitted by the relevant license (such as DTCP). Refer to the DTCP compliance [2] rules (Exhibit B). A robust cipher should be used and the key(s) used for encryption be cryptographically bound to the box so that the hard disk cannot be removed for playback on another system. More details on this approach are given in Section 7.1, "Key Management Schemes".

For details on the encryption cipher and key strength used by the media co-processor, refer to the specifications available from the manufacturer.

7.0 Secure Content Transfer Between Internal Sub-systems

For certain applications, it is necessary to transfer content streams from the media co-processor sub-system to the IA-32 memory in order to be processed by applications running on the IA-32 CPU. Previous sections of this document have already discussed the issues related to transfer of unencrypted content over the PCI bus. As mentioned, techniques to mitigate the risks of unauthorized interception may include hiding of bus traces, mini-PCI slot isolation using a PCI-to-PCI bridge and other methods. For product designs that require the flexibility of upgradeable slots on the PCI bus the content must be transferred encrypted over such buses. Again, this white paper outlines various approaches that may be considered, but the ultimate design decisions are the responsibility of the implementer, who should carefully study the specific robustness requirements associated with the technology being implemented.

Transfer of encrypted content from the media co-processor sub-system to memory buffers in the IA-32 CPU's memory space involves the following steps.

1. Key management: Software running on the media co-processor programs the processor with the key(s) for encrypting PVR content as it is stored to the hard disk drive attached to the IDE bus. The keys used to encrypt the content must also be known to the software running on the IA-32 CPU in order to be able to decrypt the encrypted content received over the PCI bus. Several options are possible and discussed in subsequent sections. For details on the encryption cipher and key strength used by the media co-processor, refer to the specifications available from the manufacturer.
2. Encrypted PVR content stored on the hard disk attached to the media co-processor must be read and transferred into IA-32 memory without being decrypted as it is read off the hard disk. The DMA transfer of data from media co-processor memory to IA-32 memory takes place over the PCI bus but the data will be encrypted and hence secure.
3. The encrypted content must then be decrypted by the application running on the IA-32 CPU before further processing. To do so, the application must have access to the same key that was used to encrypt the content.

7.1 Key Management Schemes

There are several possible options for managing keys and sharing the keys between the PVR sub-system running on the media co-processor and the software sub-system running on the IA-32 CPU. A summary of some important points to consider are given below but specific solutions are not covered in this document.

1. Both the DTCP and PHILA license compliance rules require that the content must be stored encrypted and in a manner that binds it to a single licensed product so that the encrypted content cannot be decrypted and played on another device. The key or keys used to encrypt stored content must therefore be unique to the box.
2. Secure storage of keys: Using multiple keys, such as one key to encrypt each recorded file, requires a mechanism to associate the key with the file. The keys themselves must be stored securely in non-volatile memory or within the application, protected by code obfuscation or tamper-resistant code. When the keys are stored in non-volatile memory, the keys themselves should be encrypted using a key-encryption key that is bound to the application that reads and decrypts the keys.
3. Key exchange mechanism: Because the content is encrypted and stored by software running on the media co-processor and may need to be decrypted and processed by software running on the IA-32 CPU, it is necessary for both applications to have knowledge of the key used for encrypting the content. This could be achieved by the software sub-systems at each end-point having a shared secret key or set of unique keys that are used to encrypt content stored to the hard disk. Alternatively, a secure key exchange mechanism could be employed. Specific solutions are not included in this document.

8.0 Network Security

8.1 Firewall

For receivers that have network interfaces that are connected to an IP network, the interfaces must be protected by an internal firewall. The firewall must use standard settings to protect the receiver box from well-known attacks and as otherwise required by the relevant robustness rules. TCP or UDP ports must be selectively enabled to allow only designated packets to flow through the system.

8.2 Wireless LAN Security

For designs that use wireless LAN technology such as IEEE 802.11b, 802.11a or 802.11g for distributing content from the digital media center to remote displays within the home, designers must use recommended industry standard wireless security scheme such as Wi-Fi Protected Access (WPA) and 802.11i (expected to be released by the end of 2003). See Section 9.0 for reference to a white paper released by the Wi-Fi alliance [9].

Irrespective of the underlying network security scheme, it goes without saying that content transfers must in all cases be done in accordance with the rules associated with that content and in accordance with the compliance and robustness rules associated with particular content protection and conditional access schemes. In this context, it is recommended that premium content transfers over IP networks be protected using "approved digital output technologies," such as DTCP over IP. This allows for authentication between the source and sink devices, secure transfer of data and system revocability, i.e., the ability for the licensing authority (DTLA) to revoke the licenses.

9.0 References

Number	Title	Location and Summary
1	*Content Protection System Architecture, A Comprehensive Framework for Content Protection*	http://www.4centity.com The CPSA white paper available on this site provides an overview of all the technologies for protecting content inputs and outputs.
2	*5C Digital Transmission Content Protection*	http://www.dtcp.com/ DTLA (Digital Transmission Licensing Administrator) Web site for DTCP license documents, white papers and other material related to DTCP.
3	Planning Content Protection for PC DTV, Intel Developer Update Magazine, Nov 2001	http://www.intel.com/update/departments/initech/it11012.pdf. This paper provides an overview of the elements of content security and the points of attack.
4	*Content Protection in the Digital Home*, Intel Technology Journal, Vol. 6, Nov 2002	http://www.intel.com/technology/itj/archive/2002.htm
5	*High-bandwidth Digital Content Protection (HDCP)*	http://www.digital-cp.com/
6	Advanced Encryption Standard	http://csrc.nist.gov/CryptoToolkit/aes/
7	Content Scrambling System (CSS)	DVD CCA (http://www.dvdcca.org) is the licensing authority.
8	POD-Host Interface License Agreement (PHILA)	CableLabs® OpenCable™ specifications are available on http://www.opencable.com
9	*Securing Wi-Fi Wireless Networks with Today's Technologies*	http://www.wi-fi.org/OpenSection/protected_access.asp This white paper, released by the Wi-Fi alliance, gives an overview of Wireless LAN security technologies.

§ §